North Carolina State University is a land-grant university and a constituent institution of The University of North Carolina

Department of Mathematics

NC STATE UNIVERSITY

MA 410 Theory of Numbers, second mid-semester examination, March 23, 2017

Prof. Erich Kaltofen <kaltofen@math.ncsu.edu>
www.math.ncsu.edu/~kaltofen/courses/NumberTheory/Spring17/ (URL)

919.515.8785 (phone)
919.515.3798 (fax)

Your Name: _____

For purpose of anonymous grading, please do **not** write your name on the subsequent pages.

This examination consists of 6 problems, which are subdivided into 9 questions, where each question counts for the explicitly given number of points, adding to a total of **46 points**. Please write your answers in the spaces indicated, or below the questions, using the **back of the sheets** for completing the answers and **for all scratch work,** if necessary. You are allowed to consult **two** 8.5in $\times$ 11in sheets with notes, but **not** your book or your class notes. If you get stuck on a problem, it may be advisable to go to another problem and come back to that one later.

You will have **75 minutes** to do this test.

Good luck!

Problem 1 _____

2 _____

3 _____

4 _____

5 _____

6 _____

Total _____

Problem 1 (16 points)

(a, 4pts) True or false: $\forall a \in \mathbb{Z}_{11}, a \neq 0 \colon (a^5 \bmod 11) \in \{1, 10\}$. Please explain.

(b, 4pts) True or false: $41041 = 7 \cdot 11 \cdot 13 \cdot 41$ is a Carmichael number. Please explain.

(c, 4pts) Please compute $2^{50} \bmod 25$, showing your work.

(d, 4pts) Please compute the values of the number theoretic functions $\tau(70)$, $\mu(70)$ and $\sigma(70)$.

Problem 2 (6 points): A Mersenne number is an integer of the form $2^p - 1$, where p is a prime number. Note that the Mersenne number $2^{11} - 1 = 23 \cdot 89$ is not a prime number. Please prove that the only Mersenne number that is divisible by 7 is $2^3 - 1$.

Problem 3 (6 points): Please determine an integer $n \geq 1$ such that $\phi(n) < \frac{n}{3}$, where ϕ is Euler's phi-function. Please show your work.

Problem 4 (8 points): Consider $1260 = 4 \cdot 5 \cdot 7 \cdot 9$ and let $a \in \mathbb{Z}_{1260}$ with

$$\begin{aligned} a &\equiv 3 \pmod 4, \\ a &\equiv 1 \pmod 5, \\ a &\equiv 5 \pmod 7, \\ a &\equiv 4 \pmod 9. \end{aligned}$$

Please compute $y_0 \in \mathbb{Z}_4$, $y_1 \in \mathbb{Z}_5$, $y_2 \in \mathbb{Z}_7$ and $y_3 \in \mathbb{Z}_9$ such that

$$a = y_0 + y_1 \cdot 4 + y_2 \cdot 4 \cdot 5 + y_3 \cdot 4 \cdot 5 \cdot 7.$$

Then compute a. Please show all your work.

Problem 5 (5 points): Let $k = 2^5 + 2^3 + 2^2 = 44$. Please show how one can compute $a^k \bmod n$ with 7 multiplications of residues modulo n.

Problem 6 (5 points): Please consider the RSA with the public modulus $n = pq$, where p is a prime with $p \equiv 2 \pmod 7$ (e.g., $p = 23$) and where q is a prime with $q \equiv 3 \pmod 7$ (e.g., $q = 17$), and with the public exponent $e = 7$. Please show that $d = \dfrac{3(p-1)(q-1)+1}{7}$ is an integer and that d is the private exponent for the RSA with such public moduli and public exponent 7.